GnuPG VS-Desktop - Version 3.3.0 (en)

g10 Code GmbH

2025-01-23

GnuPG VS-Desktop® version 3.3.0 is available since 2025-01-23. This release fixes a few bugs and improved the GUI. The previous version was 3.2.4.

Notes to Admins

With this version X.509 root certificates configured in the local *trustlist.txt* file are not any longer used. To revert to the former behaviour the `DisableUserTrustlist` registry entry can be set to the value "0" (see Registry keys for S/MIME). For more information on the overall configuration of root certificates see the FAQ entry on S/MIME trust.

New Features

GUI (Kleopatra)

File encryption/decryption and signing/verification

- Encryption and decryption of large files is much faster. (T6351)
- It is now possible to change the name of a decrypted file if another file with the same name already exists. (T6851)
- Files can now have multiple signatures. (T6867, T7273)
- All valid user IDs are listed for signing and encryption. This simplifies using certificates with multiple user IDs. (T7183)
- An easier to understand message is shown if a file could not be decrypted because it wasn't encrypted for one of the user's certificates. (T7295)
- An icon for folder encryption was added. (T6984)

Certificate management

- The setting whether to show tags has been removed. The tags column in the certificate lists can be shown/hidden the same way as the other columns. (T7204)
- Certificates can be updated directly from the certificate list. (T6739)
- Additional subkeys can be added to existing certificates. (T6877)
- ADSKs can be added to existing certificates. (T6879)
- Look and feel of the certificate details view has been improved. (T7019, T6924, T6959, T7128, T7227, T7229, T7237, T7250, T7258)
- Changing the validity of subkeys has been improved. (T6878, T7198)
- Generating a new OpenPGP certificate has been simplified by removing some options. (T6998)
- The confirmation window that is shown when deleting a certificate was simplified. (T7043)
- The workflow for revoking a certificate has been improved. (T7076, T7078)
- Disabled certificates are no longer listed with most filters and are ignored for operations. (T7089, T7217, T7296)
- The password protecting a subkey can be changed even if the primary secret key is not available (offline key). (T7104)
- The name of the column displaying the status of certificates (e.g. certified, not certified, expired, revoked, etc.) was changed to "Status". (T7219)
- Algorithm and keygrip can be displayed in the certificate list. (T6957)
- In the certificate details window the origin of user-IDs can be displayed. (T7096)
- Descriptions (tooltips) clarify the filter criteria that can be applied to the listed certificates. (T7302)

Certificate lookup

- Show message that certificate lookup is in progress. (T6493)
- Show the certificate details on double-click on search results. (T7027)
- Show origin in search results. (T7067)
- Show all search results if same certificate was found on multiple servers. (T7153)
- Show origin and protocol columns in search results. (T7155)
- Adapt widths of columns to search results. (T7252)
- Select a unique search result for easier import. (T6936)

Certificate groups

- The group configuration can be opened from the toolbar. (T6913)
- The configuration of groups has been simplified. (T6662, T6722, T6966, T7321)
- New groups can be created directly from the certificate list. (T6912)
- When a certificate is deleted then the groups containing the certificate are listed. (T6403)
- The group configuration is stored next to the certificates. (T6931)

Smartcard management

- Look and feel of the smartcard management has been unified. (T6420, T6847, T7018, T7082)
- Certificates are imported automatically from smartcards. (T6846)
- The workflow for moving a key to a smartcard has been improved. (T6933)

Compliance

- Ignore authentication subkeys when checking certificates for VS-NfD compliance. (T7260)

Other features

- Add option to disable OpenPGP keyserver lookup. Add option to enable automatic retrieval of signing certificates when verifying signatures. (T6950)
- Add possibility to show the GnuPG configuration to help customer support. (T6072, T7331)
- Improve accessibility of additional information offered when deleting S/MIME CA certificates. (T7073)

Outlook Add-In (GgpOL)

- New feature to handle encrypted mails processed by the Titus data classification software. This can be disabled by setting the GpgOL Registry key "disableTitusHandling" to the string value "1". (rOc1b81f8737)
- New optional feature to disable the automatic verification or decryption in the mail preview window. This feature can be enabled by setting the GpgOL Registry key "disableAutoPreview" to the string value "1". If enabled the new "Start Decryption" context menu item may be used to decrypt or verify a mail. (rO26c2fc196b)

Solved Bugs

GUI (Kleopatra)

- Ensure that links and selected certificates are readable if a high contrast color scheme is used on Windows. (T6073)
- Cancel the "print secret key" operation when the password prompt is canceled. (T6091)
- Keep selection in certificate list when showing the certificate details. (T6360)
- Always show imported certificates in a new tab. (T6447)
- Report a failed encryption if the creation of an encrypted archive is not completed successfully. (T6554)
- A crash was resolved that occurred when deleting a certificate in a circular certificate chain. (T6602)

- Do not offer publication of revocations when revoking local certifications. (T6712)
- Don't show the root certificate twice when Kleo shows a certificate chain with two certificates. (T6807)
- Create OpenPGP certificates that are created from smartcard keys with correct validity. (T6889)
- Use dark icons if the light high contrast color scheme ("Desert") is used on Windows 11. (T6921)
- Make it more obvious whether the validity of subkeys is extended together with the validity of the primary key. (T6958)
- Do not show certificate groups if no certificate in the group matches the current filter criteria. (T6970)
- Report correct reason for failure if generating smartcard keys fails because a wrong PIN is entered. (T6971)
- Also change the title of the first tab in the certificate list when the selected filter is changed. (T7002)
- Report error if lookup on server fails because of an invalid keyserver. (T7036)
- Do not perform a keyserver lookup when updating a certificate if keyserver lookup was disabled. (T7037)
- Correctly display the saved value of the "Treat .p7m files without extensions as mails" option in the configuration dialog. (T7048)
- Don't show warning that a certificate has expired for certificates that expire in the year 2038 or later. (T7069)
- Ensure that the About dialog always shows the version information for GnuPG and libgcrypt. (T7090)
- Allow showing the main window with the certificate list above the certificate details windows. (T7094)
- Show correct success/error messages when changing the reset code/PUK of an OpenPGP card. (T7122)

- Ignore leading and trailing space characters when looking up certificates on servers. (T7132)
- Do not change OpenPGP keyserver entries starting with "ldap:". (T7145)
- Do not show a success message if deleting the secret key from the hard disk fails after copying the secret key to a smart card. (T7157)
- Do not wrongly claim that a certificate without email address was updated via WKD. (T7190)
- Fix issue that the certificate details window was unusable when it was opened from the edit group window. (T7233)
- Fix a problem that occurred when importing and certifying a certificate with a revoked user ID. (T7274)
- Fix issue that the certificate details window opened in the background when opened from the decryption/verification result window. (T7244)
- Fix a problem that for some certificates the email address was shown in the Name column. (T7280)
- Fix a problem on key generation after using the "Retry" button. (T7365)
- A crash was resolved that occurred when unplugging a smartcard while an operation is in progress. (T7372)
- Correctly finish a print secret key operation if an empty or wrong password is entered. (T7375)
- Ensure that tool tips are easy to read if a dark color scheme is used on Windows. (T7414)

Engine (GnuPG)

- gpg: Add the AEAD algo number to the DECRYPTION_INFO status line. (T7398)
- gpg: Allow the use of an ADSK subkey as ADSK subkey. (T6882)
- gpgtar: Make sure to create upper directories for regular files. (T7380)
- agent: Fix status output for LISTTRUSTED. (T7363)

Outlook Add-In (GgpOL)

- A crash was resolved that sometimes occurred in the security approval window and that resulted in a "No recipients for encryption selected" error in Outlook. (T7312)
- Fixed a crash on certain mails. (rO34d53b4309)
- Fix setting of the content-id when sending multipart/related. (T5982)
- Don't show conformance status if "Do not sign this email" is selected in the security approval window. (T6808)

Versions of the Components

Component	Version	Remarks
GnuPG	2.2.46	T7314
Kleopatra	3.3.0	
GpgOL	2.5.15	
GpgEX	1.0.11	
Libgcrypt	1.8.11	T6335
Libksba	1.6.7	T7173